



State of North Dakota
Information Technology Department
Hosting Service Levels

Purpose

This document outlines the characteristics of North Dakota's Hosting service. In conjunction with ITD's [Enterprise Service Levels](#)¹, it acts as a Service Level Agreement between the ND Information Technology Department (ITD) and all customers that utilize the Hosting service.

Service Description

ITD offers an environment for hosting enterprise services and line-of-business systems. It provides operational and infrastructure support that includes, but is not limited to, the following components:

Facilities

- A professional, raised floor datacenter equipped with redundant cooling and conditioned power which is supported by a UPS and diesel generator.
- Physical security is provided via a key card system with all access logged and monitored.
- Facilities comply with the [Enterprise Architecture Physical Access Security Standard](#)².

Hardware

- Solutions provided include rack space and professional-class server equipment designed for maximum availability with redundant components.
- Hardware is acquired with vendor supplied warranty and support.
- Hardware typically follows a 4-year replacement cycle.
- When appropriate, shared or virtual hardware is used in order to minimize costs.
- Hardware will be installed and configured in compliance with industry best-practices.
- Firmware updates will be installed as needed.

Operating Systems

- Distributed solutions are supported on multiple platforms in accordance with the [Enterprise Architecture Server Operating Systems Standard](#)³.
- Anti-virus protection is provided in compliance with the [Enterprise Architecture Anti-Virus Standard](#)⁴.

Storage

- ITD provides sufficient storage for operating systems, application software, and log files. Customers are generally billed by volume for application data.

Monitoring & Alerting

- ITD provides proactive monitoring of databases and hosted applications to ensure they are available for login. Customers must notify ITD if more extensive "beyond the application login" monitoring is required.
- Alerts are automatically reported as incidents to ITD's Service Desk on a 24x7 basis. Each incident is assigned a priority that drives ITD's resource commitment.

Load Testing & Performance Tuning

- All line-of-business web applications (written by ITD or purchased from a vendor) that run on shared ITD infrastructure must be load tested prior to production use in order to avert the risk of degrading server performance. ITD uses a variety of factors to ultimately determine if an application is performing at an acceptable level.

Load tests are performed prior to initially loading an application into production and prior to reloading a modified application into production. Cosmetic changes are exempt from the load testing requirement. ITD may also request load testing when upgrading infrastructure components, such as hardware or operating systems. Rates for load testing are variable and will be based on the number of estimated users for the application.

- ITD monitors the performance metrics of the application environment and tunes the infrastructure for maximum performance and availability.

Availability

Ideally, availability should be measured end-to-end for an application within scheduled hours of operation. This approach is preferred over measuring individual components, such as database, network, and server availability, which would *each* have to be considerably higher to meet end-to-end levels.

ITD has the capability of providing end-to-end application monitoring for customers that are willing to incur scripting and licensing expenses. For all other services, uptime is determined by measuring the availability of a cluster of critical components and/or login pages.

The following assessment shows industry levels of high availability and hours of unplanned downtime. It is based upon a whitepaper published by Gartner, Inc. on April 23, 2009. The figures exclude planned downtime, which is agreed to by the customer in advance. Service disruptions caused by circumstances out of ITD's control (including deficiencies in vendor/customer software or acts of nature) may also be reported as a separate category.

Category	Availability Metrics	24 x 7 Unplanned Downtime		Primary Business Hours ¹ Unplanned Downtime	
		Annually	Monthly	Annually	Monthly
Baseline ²	98.50%	131 hours	11 hours	34 hours	3 hours
Good ³	99.00%	88 hours	7 hours	22 hours	2 hours
Very Good ⁴	99.30%	61 hours	5 hours	16 hours	1.3 hours
Outstanding ⁴	99.70%	26 hours	2 hours	7 hours	35 minutes
Best in Class ⁴	99.95%	4 hours	20 minutes	1 hour	5 minutes

¹ Primary Business Hours are 8am-5pm CDT, Monday through Friday; excluding state holidays

² Defined by ITD as the minimum threshold of acceptable service availability

³ Defined by ITD as a historically achievable level of service availability

⁴ Defined by Gartner, Inc. as a category of high-availability

ITD often provides what Gartner defines as *Very Good*, *Outstanding* and even *Best in Class* service. However, specific IT architecture and infrastructure is required to ensure consistent availability at these levels. Customers must inform ITD of any application that requires critical or highly-critical levels of availability; by default, most applications are not architected in this fashion. Budgetary constraints typically constrain critical and highly-critical designations to systems that support public safety, health, finance, and/or legal obligations. Rates will be determined on a case-by-case basis.

Short and frequent outages could potentially cause availability metrics to appear adequate even as customer satisfaction declines. Therefore, the number of unexpected outages for a particular service must also be considered.

Through best-effort support and component redundancy:

- General government services typically achieve at least 99.00% (*Good*) to 99.3% (*Very Good*) availability and experience two or less unexpected outages per month within business hours.

Through a highly-available architecture (requested and funded by customers):

- Critical applications are designed to achieve at least 99.7% availability with one or less unplanned outage per month within scheduled hours of operation.
- Highly-critical applications are designed to achieve at least 99.95% availability with four or less unplanned outages per year within scheduled hours of operation.

Data Backup

ITD provides data backup in accordance with the [Enterprise Architecture Electronic Data Backup Standard](#)⁵. Data backups can cause significant load on system resource and measurably impact normal business operations. Therefore, the time for backups should be planned and agreed upon. Generally speaking:

- Daily off-site backups are provided for all data hosted and source-code written by ITD. Databases have full weekly backups and nightly incremental backups, while other datasets only backup items that have changed during the day.
- Standard backup configuration allows for a maximum of five different versions of each file to be stored within a 17 day window. A single version of the file will be retained even if it was done outside the 17 day window. Upon deletion from a system, the most recent version of a file is retained for 47 days before being completely purged from backup. Large-scale storage of static data typically warrants an alternative custom backup configuration.
- Data backups are optimized for Disaster Recovery purposes and are not intended to be used for records retention.

Service level objectives for backup reliability include:

- There will be less than two failed/cancelled full or incremental backups per month
- Successful backups are expected 99.00% of the time, with a minimum of 95.00%
- Successful recoveries are expected 99.00% of the time, with a minimum of 95.00%

System Recovery

All hosted systems are designed with disaster recovery requirements as determined by the customer's business needs. Therefore, it is the customer's responsibility to notify ITD of any specific disaster recovery requirements that exist. Custom disaster recovery configurations are available upon request.

Due to cost, most hosted applications are not architected for high-availability and/or business continuity. By default:

- A very limited amount of spare hardware is available. If replacement hardware needs to be ordered, extended outages should be expected.
 - Agencies that do not invest in replicated data solutions and redundant processing capacity will need to wait for additional storage and servers to be procured and provisioned. The estimated Recovery Time Objective (RTO) for production systems is 3-8 weeks; depending on hardware availabilities, staffing priorities, and amount of data to be restored from backup.
 - Agencies that invest in replicated data solutions but do not invest in redundant processing capacity will need to wait for servers to be procured and provisioned. The estimated RTO for production systems is 2-4 weeks; depending on hardware availability and staffing priorities. Note that some agencies have test and/or development environments residing in the secondary datacenter that could be provisioned for production use in the event of a disaster.
- In the event of a disaster, ITD will put forth its *best-effort* to restore service in a timely manner and to keep customers informed of progress. Customers will retain responsibility for restoring associated end-user devices.

A very limited subset of ITD hosting services have been architected for business continuity within their base rate. Specifically:

- Email, file server, and the AS/400 (iSeries) platform have an RTO of one hour
- The mainframe (zSeries), DELA, and ConnectND environments have an RTO of 4-12 hours
- Website content on the enterprise Drupal Content Management System has an RTO of 1-2 hours. This does not inherently include applications launched from static pages.

Database and System Administration

ITD supports databases on multiple platforms in accordance with the [Enterprise Architecture Databases Standard](#)⁶, the [Enterprise Architecture Enterprise Database Security Standard](#)⁷, and the [Enterprise Architecture Database Security Best Practices](#)⁸.

ITD is responsible for creating all User-IDs and database schemas in development, test, and production environments. ITD is also responsible for any structure changes in production and test environments, including:
























































- Creation of table-spaces, redo logs, and control files.
- Configuration of database parameters.
- Application of upgrade scripts.

Customers and their vendor(s) are encouraged to work closely with ITD's database administrators and security analysts when deploying and securing databases. In development and test environments, customers that are not utilizing ITD's Software Development staff are responsible for:

- Data modeling designs.
- Creation of schema database objects, including tables, views, indexes, procedures, triggers, functions, etc.
- Database tuning and performance testing before deployment to test and/or production.
- Setting up application and database security, and testing before deploying to production. This includes creating database roles and granting object privileges to roles.
- Monitoring batch processing jobs.

Customers shall contact ITD's Service Desk if the installation of an operating system or security patch is known to have an adverse impact on their application(s). The customer shall assume all risk associated with *not* installing the patch.

Production, test, and development environments do not inherently exist for all systems. When applicable, ITD is responsible for staging applications from Test to Production.

	Production			Test			Development		
	Primary Hours ¹	Extended Hours ²	After Hours ³	Primary Hours ¹	Extended Hours ²	After Hours ³	Primary Hours ¹	Extended Hours ²	After Hours ³
Response to high-priority automated alerts ⁴								No	No
Recovery and restoration of backups								No	No
Instance restarts to restore availability								No	No
Instance restarts to implement planned changes ⁵						No			No
Patches and upgrades						No			No
Planned changes						No			No
Emergency changes ⁶						No			No
Meeting attendance		No	No		No	No		No	No
Consulting and advise ⁷		No	No		No	No		No	No

¹ Primary Hours: Monday – Friday, 8:00 AM to 5:00 PM

² Extended Hours: Monday – Friday, 7:00 AM to 8:00 AM and 5:00 PM to 10:00 PM

³ After Hours: Saturday, Sunday, Holidays, and Monday – Friday from 10:00 PM to 7:00 AM

⁴ Charges may apply to after-hour support if caused by user action or departmental coding errors.

⁵ Database restarts during primary and extended business hours are included in the standard rate. However, charges may apply if business requirements mandate after-hour database restarts.

⁶ Emergency changes during extended and after hours will be reviewed on a case-by-case basis to determine billing action.

⁷ Extensive engagements may be charged a standard hourly rate.

Consent

On June 12, 2013, Information Technology Department and the Enterprise Architecture Review Board agreed to the terms of this document.

Modifications Pending Mutual Approval

Date	SLA Modification
2010-06-22	Changed document title from "Hosting" to "Hosting Service Levels"
2010-06-25	Updated ITD logo and added "State of North Dakota" / "Information Technology Department" to header
2010-06-25	Added hyperlinks/ endnotes to "Enterprise Service Levels"
2011-01-07	Redirected hyperlinks/endnotes to content on ITD's new website
2011-04-06	In Consent section, update the agreement date to March 9, 2011
2012-08-08	Significantly revised the Business Continuity section to more clearly articulate the current state
2013-02-05	Moved general Business Continuity into the Enterprise Service Level Agreement
2014-12-18	Redirected hyperlinks/endnotes to correspond with URL restructuring of EA standards
2015-04-13	Add RTO for Drupal Content Management System
2015-10-19	Redirected hyperlinks/endnotes to content on ITD's new website

Endnotes

- ¹ <http://www.nd.gov/itd/sites/itd/files/legacy/sla/sla-enterprise.pdf>
- ² <https://www.nd.gov/itd/standards/physical-access>
- ³ <https://www.nd.gov/itd/standards/server-operating-systems>
- ⁴ <https://www.nd.gov/itd/standards/anti-virusmalware>
- ⁵ <https://www.nd.gov/itd/standards/electronic-data-backup>
- ⁶ <https://www.nd.gov/itd/standards/databases>
- ⁷ <https://www.nd.gov/itd/standards/enterprise-database-security>
- ⁸ <https://www.nd.gov/itd/standards/database-security-best-practices>